Sottung Security Consulting
Informationssicherheit & Resilienz

ISMS

ISMS-Startpaket
Ein ISMS aufbauen, das im Alltag trägt

Kurzleitfaden aus der Prüferpraxis: acht Schritte, realistischer Zeitplan, Checkliste der Pflichtdokumente nach ISO 27001 und ein Selbstcheck zum Ausfüllen.

Jürgen Sottung
KRITIS-Auditor · ISO 27001 Lead Auditor · externer ISB

Stand: November 2026
ssc-ism.de

EINORDNUNG

Was ein ISMS ist – und was nicht

Ein Informationssicherheits-Managementsystem (ISMS) ist kein Software-Produkt und kein Ordner voller Richtlinien. Es ist die Art, wie eine Organisation Informationssicherheit steuert: mit klaren Verantwortlichkeiten, bewerteten Risiken, umgesetzten Maßnahmen und einem Kreislauf aus Prüfen und Verbessern.

ISO/IEC 27001

Internationale Norm. Legt fest, **was** ein ISMS leisten muss, und lässt bei den Maßnahmen viel Spielraum – die Auswahl folgt aus der eigenen Risikobewertung. Zertifizierbar, international anerkannt, häufig von Kunden gefordert.

BSI IT-Grundschutz

Methodik des BSI (BSI-Standards 200-1 bis 200-3). Gibt mit seinen Bausteinen deutlich konkreter vor, **wie** typische Systeme und Prozesse abzusichern sind. Verbreitet in Behörden und im öffentlichen Umfeld.

Beide Wege führen zu einem funktionierenden ISMS. Welcher besser passt, hängt von Kunden, Aufsicht und Ausgangslage ab – der grundlegende Ablauf ist in beiden Fällen ähnlich.

Warum gerade jetzt?

- **NIS-2:** Besonders wichtige und wichtige Einrichtungen müssen nach § 30 BSIG geeignete, verhältnismäßige und wirksame Risikomanagementmaßnahmen umsetzen und deren Einhaltung dokumentieren. Ein ISMS ist der Rahmen, in dem das gelingt.
- **Kunden und Lieferkette:** Immer mehr Auftraggeber verlangen Nachweise zur Informationssicherheit – oft eine ISO-27001-Zertifizierung oder eine vergleichbare Selbstauskunft.
- **Geschäftsleitung:** Die Verantwortung für Informationssicherheit liegt bei der Leitung. Ein ISMS macht sichtbar, welche Risiken bestehen und wie mit ihnen umgegangen wird.

Wichtig vorab

NIS-2 schreibt keine Zertifizierung vor. Ein ISMS kann auch ohne Zertifikat aufgebaut und betrieben werden. Entscheidend ist, dass es im Alltag wirkt – und dass sich das nachweisen lässt.

VORGEHEN

Acht Schritte – ein Kreislauf, kein Projekt



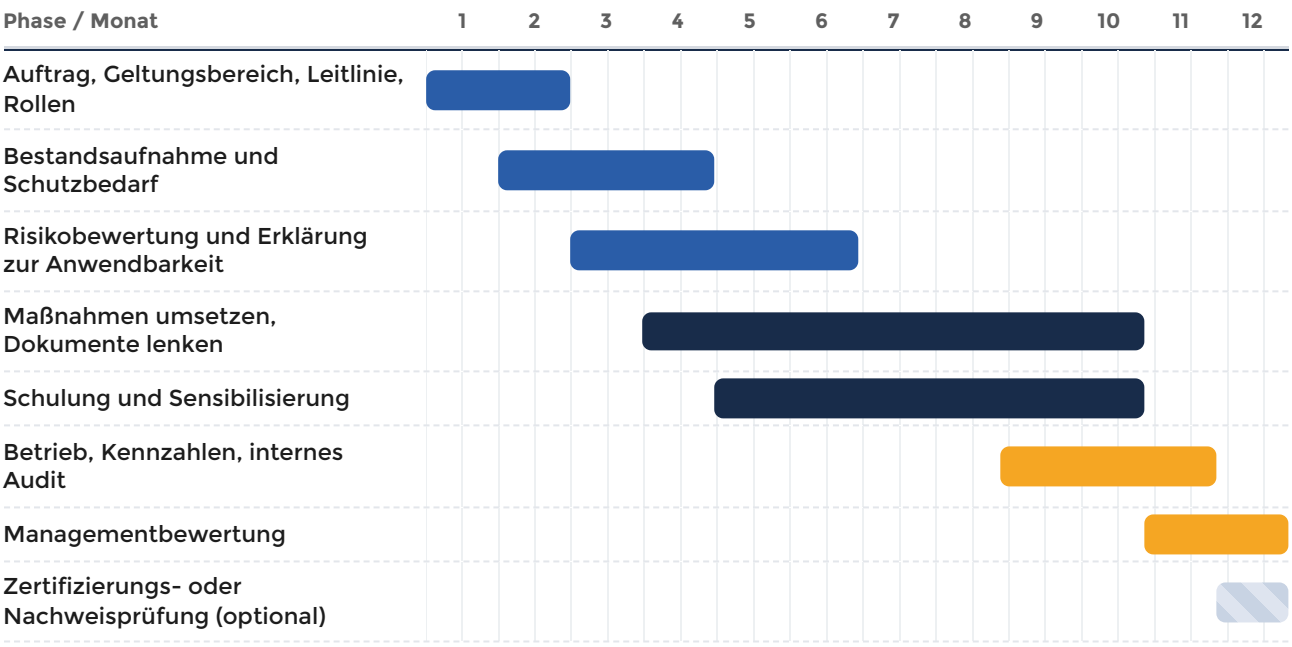
1. **Auftrag der Leitung:** Die Geschäftsleitung beschließt den Aufbau, stellt Zeit und Budget bereit und übernimmt die Verantwortung.
2. **Geltungsbereich:** Welche Standorte, Prozesse, Systeme und Dienstleister gehören dazu? Nicht zu eng, nicht zu weit.
3. **Leitlinie und Rollen:** Informationssicherheitsleitlinie, freigegeben von der Leitung; ein ISB und klar geregelte Zuständigkeiten.
4. **Bestandsaufnahme:** Informationen, Prozesse, Anwendungen, Systeme und Dienstleister (Assets) und ihr Schutzbedarf.
5. **Risiken bewerten und behandeln:** Maßnahmen festlegen, Restrisiken bewusst akzeptieren. Ergebnis bei ISO 27001: die Erklärung zur Anwendbarkeit (SoA).
6. **Maßnahmen umsetzen:** Richtlinien, Prozesse und Technik einführen; Dokumente lenken – mit Verantwortlichem, Version und Freigabe.
7. **Schulen und sensibilisieren:** Alle kennen die Regeln, die für sie gelten, und wissen, wie sie Vorfälle melden.
8. **Betreiben, prüfen, verbessern:** Kennzahlen, internes Audit und Managementbewertung. Erst dieser Kreislauf (KVP) macht aus Dokumenten ein Managementsystem.

PLANUNG

Wie lange dauert der Aufbau?

Als Erfahrungswert erreichen kleine und mittlere Organisationen mit einer engagierten Leitung und einem festen Ansprechpartner die Zertifizierungs- oder Prüfungsreife häufig in sechs bis zwölf Monaten.

Das folgende Beispiel zeigt einen typischen Ablauf über zwölf Monate. Phasen überlappen bewusst: Maßnahmen beginnen, sobald die ersten Risiken bewertet sind.



Was den Aufbau beschleunigt

- Leitung, die Entscheidungen zügig trifft
- fester interner Ansprechpartner mit Zeitbudget
- aktuelles Inventar und geregelte Berechtigungen
- Standortbestimmung zu Beginn

Was ihn verzögert

- ISMS „neben dem Tagesgeschäft“ ohne Zeitbudget
- fehlende Grundstrukturen (Inventar, Rollen)
- Abstimmungsschleifen ohne Entscheider
- zu weit gefasster erster Geltungsbereich

Der größte Aufwand liegt selten in den Dokumenten, sondern in der Abstimmung mit den Fachbereichen und in der Umsetzung der Maßnahmen.

CHECKLISTE ZUM ABHAKEN

Pflichtdokumente nach ISO/IEC 27001:2022

Die Norm verlangt eine Reihe dokumentierter Informationen. Die wichtigsten im Überblick:

	DOKUMENT / NACHWEIS	ABSCHNITT
☐	Geltungsbereich des ISMS	4.3
☐	Informationssicherheitsleitlinie	5.2
☐	Verfahren zur Risikobewertung	6.1.2
☐	Verfahren zur Risikobehandlung	6.1.3
☐	Erklärung zur Anwendbarkeit (Statement of Applicability, SoA)	6.1.3 d
☐	Informationssicherheitsziele	6.2
☐	Nachweise der Kompetenz	7.2
☐	Dokumentierte Information zur Steuerung der Prozesse	8.1
☐	Ergebnisse der Risikobewertung	8.2
☐	Ergebnisse der Risikobehandlung	8.3
☐	Ergebnisse von Überwachung und Messung	9.1
☐	Auditprogramm und Auditergebnisse	9.2
☐	Ergebnisse der Managementbewertung	9.3
☐	Nichtkonformitäten und Korrekturmaßnahmen	10.2

Typische weitere Dokumente aus den Maßnahmen (Anhang A)

Je nach Risikobewertung, zum Beispiel: Inventar der Werte, Zugangs- und Berechtigungskonzept, Backup- und Wiederherstellungskonzept, Notfall- und Vorfallmanagement, Lieferanten- und Dienstleistersteuerung, Regeln zur zulässigen Nutzung, Schulungs- und Sensibilisierungsplan.

> **Aus der Prüferpraxis:** Mehr Dokumente bedeuten nicht mehr Sicherheit. Im Audit zählt, dass Dokumente gelten, bekannt sind, gelenkt werden – und eingehalten werden.

AUS DER PRÜFERPRAXIS

Woran der ISMS-Aufbau scheitert

Selten an der Norm – fast immer am Alltag. Was geplant ist, und was im Audit tatsächlich zu sehen ist:

ANSPRUCH	ALLTAG IM AUDIT
Eigene, passende Dokumentation	Gekaufte Vorlagen, die nicht zur Organisation passen
ISMS für die ganze Organisation	Personal, Einkauf und Gebäude bleiben außen vor
Risiken führen zu Entscheidungen	Tabelle ausgefüllt – niemand entscheidet
ISMS läuft das ganze Jahr	Nach dem Audit ruht alles bis zum nächsten
ISB mit Zeit und Mandat	Der ISB macht es „nebenbei“

Ein schlankes ISMS, das betrieben wird, schlägt ein umfangreiches im Schrank.

ssc-ism.de

Woran ich ein gelebtes ISMS erkenne

- Die Leitung kennt die wichtigsten Risiken – ohne nachzuschlagen.
- Maßnahmen haben Verantwortliche und Termine.
- Abweichungen aus dem letzten Audit sind tatsächlich bearbeitet.
- Ausnahmen sind dokumentiert, begründet und befristet.

SELBSTCHECK ZUM AUSFÜLLEN

Wo steht Ihr ISMS?

Kreuzen Sie für jede Aussage an, was am ehesten zutrifft.

	Aussage	Ja	Teilweise	Nein
Rahmen und Verantwortung				
1	Die Geschäftsleitung hat das ISMS beauftragt und eine Leitlinie freigegeben.	☐	☐	☐
2	Der Geltungsbereich ist schriftlich festgelegt und deckt die wichtigsten Prozesse ab.	☐	☐	☐
3	Es gibt einen ISB mit festem Zeitbudget und direktem Zugang zur Leitung.	☐	☐	☐
Risiken und Maßnahmen				
4	Ein aktuelles Inventar der Informationen, Systeme und Dienstleister liegt vor.	☐	☐	☐
5	Risiken sind bewertet, und über Maßnahmen und Restrisiken wurde entschieden.	☐	☐	☐
6	Maßnahmen haben Verantwortliche und Termine, deren Umsetzung wird verfolgt.	☐	☐	☐
7	Dienstleister mit Zugriff auf Systeme oder Daten werden gesteuert und vertraglich verpflichtet.	☐	☐	☐
Betrieb und Nachweis				
8	Richtlinien sind gelenkt (Version, Freigabe) und den Betroffenen bekannt.	☐	☐	☐
9	Beschäftigte werden regelmäßig geschult und wissen, wie sie Vorfälle melden.	☐	☐	☐
10	Backup und Wiederherstellung werden regelmäßig getestet.	☐	☐	☐
11	Ein internes Audit hat in den letzten zwölf Monaten stattgefunden.	☐	☐	☐
12	Die Leitung bewertet das ISMS mindestens jährlich und trifft Entscheidungen daraus.	☐	☐	☐

Überwiegend „Ja“

Gute Basis. Prüfen Sie, ob das ISMS auch einem unabhängigen Blick standhält – etwa mit einem Probeaudit.

Viel „Teilweise“

Die Struktur steht, der Betrieb hakt. Meist fehlen Zeit, Entscheidungen oder die Nachverfolgung.

Mehrere „Nein“

Starten Sie mit Schritt 1 bis 3 – Auftrag, Geltungsbereich, Rollen – und einer Standortbestimmung.

NÄCHSTE SCHRITTE

Vom Startpaket zum gelebten ISMS

Sottung Security Consulting begleitet Organisationen beim Aufbau und Betrieb von Informationssicherheit – mit dem Blick eines Prüfers, der weiß, worauf es im Audit ankommt.

SSC Kompass

Standortbestimmung und NIS-2-Betroffenheitsprüfung mit dokumentiertem Ergebnis und Gap-Analyse.

SSC Fundament

ISMS aufbauen nach ISO 27001 oder BSI IT-Grundschutz – bis zur Zertifizierungs- bzw. Prüfungsreife.

SSC Lotse

Externer Informationssicherheitsbeauftragter: ISMS-Betrieb, Risikomanagement und Reporting an die Leitung.

Kostenfreies Kennenlerngespräch

30 Minuten per Microsoft Teams: Sie schildern kurz Ihre Ausgangslage, wir klären gemeinsam den sinnvollsten nächsten Schritt. Unverbindlich – den Termin wählen Sie direkt online.

Termin wählen: ssc-ism.de/kontakt

E-Mail: info@ssc-ism.de · LinkedIn: linkedin.com/in/juergensottung

Sottung Security Consulting
Informationssicherheit & Resilienz

Jürgen Sottung – KRITIS-Auditor, ISO 27001 Lead Auditor und externer ISB. Über 25 Jahre IT-Management als Führungskraft, heute auf der Seite der Prüfung und Beratung.

Weiterlesen

- ISMS aufbauen: Schritte, Dauer und typische Stolpersteine
- NIS-2: Bin ich betroffen? Die Prüfung in drei Schritten
- Brauche ich für NIS-2 eine ISO-27001-Zertifizierung?

Stand: November 2026. Dieser Leitfaden gibt einen allgemeinen Überblick aus der Praxis und ersetzt keine Rechts- oder Einzelfallberatung. Quellen: ISO/IEC 27001:2022; BSI-Standards 200-1 bis 200-3; § 30 BSIG. © Sottung Security Consulting – Weitergabe in unveränderter Form ausdrücklich erwünscht.